I Claim:

1    1.    A system for authenticating a key of a user, comprising a

2    decrypt engine for decrypting an encrypted data file provided by the

3    user with a password provided by the user into the key of the user.


1    2.    The system of claim 1, wherein the encrypted data file is stored

2    on a RF smart card.


1    3.    The system of claim 1, wherein the encrypted data file contains

2    encrypted biometric data identifying the user.


1    4.    The system of claim 3, wherein the biometric data includes a

2    digitized fingerprint of the user.


1    5.    The system of claim 3, further including a scanned biometric

2    reading of the user, wherein the scanned biometric reading of the user

3    is probabilistically compared with the key of the user in order to

4    additionally authenticate the key of the user.


1    6.    The system of claim 5, wherein the scanned biometric reading of

2    the user is a fingerprint scan.

1  7.    A method for providing an authenticated key of a user,

2  comprising the steps of:

3        providing an encrypted data file;

4        providing a password; and

5        decrypting the encrypted data file using the password into an

6  authenticated key of the user.


1  8.    The method of claim 7, wherein the encrypted data file is stored

2  an a RF smart card.


1  9.    The method of claim 7, wherein the encrypted data file contains

2  encrypted biometric data identifying the user.


1  10.   The method of claim 9, wherein the biometric data includes a

2  digitized fingerprint of the user.


1  11.   The method of claim 9, further including the steps of:

2        scanning a biometric feature of the user; and

3        probabilistically comparing the scanned biometric feature of the

4  user with the key of the user in order to additionally authenticate the

5  key of the user prior to securely transmitting data using the key.


1  12.   The method of claim 11, wherein the scanned biometric feature

2  of the user is a fingerprint.

1    13.    A computer-readable medium comprising program instructions

2    for providing an authenticated key of a user, comprising the step of:

3          decrypting an encrypted data file provided by the user using a

4    password provided by the user into an authenticated key of the user.